

# Further results on constructions of generalized bent Boolean functions

Fengrong ZHANG<sup>1</sup>, Shixiong XIA<sup>1\*</sup>, Pantelimon STĂNICĂ<sup>2</sup> & Yu ZHOU<sup>3</sup>

<sup>1</sup>*School of Computer Science and Technology, China University of Mining and Technology, Xuzhou 221116, China;*

<sup>2</sup>*Naval Postgraduate School, Applied Mathematics Department, Monterey, CA 93943, USA;*

<sup>3</sup>*Science and Technology on Communication Security Laboratory, Chengdu 610041, PR China*

Received ; accepted

**Citation** Zhang F R, Xia S X, Stănică P, et al. Further results on constructions of generalized bent Boolean functions. *Sci China Inf Sci*, 2016, 59(3): \*\*\*\*\*, doi: \*\*\*\*\*

Dear editor,

Boolean bent functions were introduced by Rothaus in 1976 as an interesting combinatorial object with the important property of having optimal nonlinearity [1]. Since bent functions have many applications in sequence design, cryptography and algebraic coding, they have been extensively studied during the last thirty years [2, 3]. Over the past decades, based on bent functions, several constructions of highly nonlinear balanced functions were presented [4, 5].

In recent years several researchers have proposed generalizations of Boolean functions [6–9] and studied the effect of the Walsh-Hadamard transform on these classes. In [6], Schmidt presented the connection between words in multi-code code-division multiple access (MC-CDMA) systems and generalized bent functions from  $\mathbb{Z}_2^m$  to  $\mathbb{Z}_4$ , and considered functions from  $\mathbb{Z}_2^n$  to  $\mathbb{Z}_q$  from the viewpoint of cyclic codes over rings. Later, Solé and Tokareva [7] called these functions from  $\mathbb{Z}_2^n$  to  $\mathbb{Z}_q$  generalized Boolean functions and presented the direct links between Boolean bent functions and generalized bent functions. More recently, Stănică et al. [9] investigated the properties of generalized bent functions and presented several constructions of such generalized bent functions

for both  $n$  even and  $n$  odd. They characterized a class of generalized bent functions symmetric with respect to two variables and generalized bent functions defined on  $\mathbb{Z}_2^n$  in  $\mathbb{Z}_8$ . However, is there a technique that provides generalized bent functions symmetric with respect to  $m$  variables, where  $m$  is even? Additionally, in [9, Example 20, 21] the authors provided an explicit construction only for the even case. These give us a motivation to identify those generalized bent functions.

Let us denote the set of integers, real numbers and complex numbers by  $\mathbb{Z}, \mathbb{R}$  and  $\mathbb{C}$ , respectively and let the ring of integers modulo  $r$  be denoted by  $\mathbb{Z}_r$ . We denote the addition over  $\mathbb{Z}, \mathbb{R}$  and  $\mathbb{C}$  by ‘+’. Moreover, addition modulo  $q$  ( $\neq 2$ ) is also denoted by ‘+’ and it is understood from the context. Let  $\mathbb{Z}_2^n$  be the  $n$ -dimensional vector space over  $\mathbb{Z}_2$ . We denote the addition over  $\mathbb{Z}_2^n$  and  $\mathbb{Z}_2$  by ‘ $\oplus$ ’. Letting  $\omega = (\omega_1, \dots, \omega_n)$  and  $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{Z}_2^n$ , we define the inner (or scalar) product by  $\omega \cdot \mathbf{x} = \omega_1 x_1 \oplus \dots \oplus \omega_n x_n$ . If  $z = a + bi \in \mathbb{C}, a, b \in \mathbb{R}$ , then  $|z| = \sqrt{a^2 + b^2}$  denotes the absolute value of  $z$ , where  $i^2 = -1$ . We denote the vectors  $(0, 0, \dots, 0) \in \mathbb{Z}_2^n$  by  $\mathbf{0}_n$ .

A function from  $\mathbb{Z}_2^n$  to  $\mathbb{Z}_q$  ( $q \geq 2$  a positive integer) is called a *generalized Boolean function* in  $n$  variables [7]. Let  $\mathcal{GB}_n^q$  be the set of all  $n$ -variable

\* Corresponding author (email: xiasx@cumt.edu.cn)

The authors declare that they have no conflict of interest.

generalized Boolean functions from  $\mathbb{Z}_2^n$  to  $\mathbb{Z}_q$ . If  $q = 2$ , we obtain the classical Boolean functions in  $n$  variables, whose set will be denoted by  $\mathcal{B}_n$ . The *Hamming weight*  $\text{wt}(\mathbf{u})$  of a vector  $\mathbf{u} \in \mathbb{Z}_2^n$  is the weight (number of 1's) of the binary string.

The (generalized) *Walsh-Hadamard transform* of  $f \in \mathcal{GB}_n^q$  is the complex valued function over  $\mathbb{Z}_2^n$  which is defined by  $\mathcal{H}_f(\boldsymbol{\omega}) = \sum_{\mathbf{x} \in \mathbb{Z}_2^n} \zeta^{f(\mathbf{x})} (-1)^{\mathbf{x} \cdot \boldsymbol{\omega}}$  where  $\zeta (= e^{2\pi i/q})$  is the complex  $q$ -primitive root of unity. When  $q = 2$ , we obtain the Walsh transform of  $f \in \mathcal{B}_n$ , which will be denoted by  $\mathcal{W}_f$ .

A generalized Boolean function  $f \in \mathcal{GB}_n^q$  is called *generalized bent* (or *gbent*, for short) if and only if  $|\mathcal{H}_f(\boldsymbol{\omega})| = 2^{n/2}$  for all  $\boldsymbol{\omega} \in \mathbb{Z}_2^n$ . Note that when  $q = 2$ , Boolean bent functions exists only if the number  $n$  of variables is even. For  $q > 2$ , if  $f$  is a gbent function in  $n$  variables, it does not follow that  $n$  must be even. Such functions for  $q = 4$  were investigated by Schmidt [6], Solé and Tokareva [7], Stănică, Martinsen, Gangopadhyay, and Singh [9], etc.

The sum  $\mathcal{C}_{f,g}(\mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{Z}_2^n} \zeta^{f(\mathbf{x}) - g(\mathbf{x} \oplus \mathbf{u})}$  is the *crosscorrelation* of  $f$  and  $g$  at  $\mathbf{u} \in \mathbb{Z}_2^n$ . The *autocorrelation* of  $f \in \mathcal{GB}_n^q$  at  $\mathbf{u} \in \mathbb{Z}_2^n$  is  $\mathcal{C}_{f,g}(\mathbf{u})$  above, which is denoted by  $\mathcal{C}_f(\mathbf{u})$ .

**Lemma 1.** Let  $f \in \mathcal{GB}_n^q$ . Then  $f$  is a gbent function if and only if

$$\mathcal{C}_f(\mathbf{u}) = \begin{cases} 2^n, & \text{if } \mathbf{u} = \mathbf{0}_n, \\ 0, & \text{if } \mathbf{u} \neq \mathbf{0}_n. \end{cases}$$

By using Lemma 1, we can prove the following theorem.

**Theorem 1.** Let  $n$  be a positive integer and  $m, q$  be even positive integers. Let  $f \in \mathcal{GB}_n^q$  be gbent. Let  $f + \frac{q}{2}g_i \in \mathcal{GB}_n^q$  be gbent, where  $i = 0, 1$ . Let  $\mathbf{y} = (\mathbf{y}', \mathbf{y}'')$ ,  $\mathbf{y}' = (y_1, y_2, \dots, y_{m/2})$ ,  $\mathbf{y}'' = (y_{m/2+1}, y_{m/2+2}, \dots, y_m)$  and  $\vartheta(\mathbf{y}) = \mathbf{y}' \cdot \mathbf{y}''$ . Let  $\mathbf{c} \in \mathbb{Z}_2^m$  and  $\text{wt}(\mathbf{c})$  be even. Then the function  $h \in \mathcal{GB}_n^q$ , defined by

$$h(\mathbf{x}, \mathbf{y}) = f(\mathbf{x}) + \frac{q}{2}(\mathbf{c} \cdot \mathbf{y})g_{\mathbf{c} \cdot \mathbf{y}}(\mathbf{x}) + \frac{q}{2}\vartheta(\mathbf{y}) \quad (1)$$

is a gbent function in  $n + m$  variables.

In Table 1, we compare our approach to other methods [9, 10] in terms of the form of gbent functions.

In what follows, we first provide some notations.

If  $f \in \mathcal{B}_n$  is bent, then the dual function  $\tilde{f}$  of  $f$ , defined on  $\mathbb{Z}_2^n$  by  $\mathcal{W}_{\tilde{f}}(\boldsymbol{\omega}) = 2^{n/2}(-1)^{\tilde{f}(\boldsymbol{\omega})}$  is also bent and it is known that  $\tilde{\tilde{f}} = f$ .

**Lemma 2.** For every  $\mathbf{a}, \mathbf{b} \in \mathbb{Z}_2^n$  and for every bent function  $f$ , the dual of the function  $f(\mathbf{x} \oplus \mathbf{b}) \oplus \mathbf{a} \cdot \mathbf{x}$  equals  $\tilde{f}(\mathbf{x} \oplus \mathbf{a}) \oplus \mathbf{b} \cdot (\mathbf{x} \oplus \mathbf{a})$ .

The original Maiorana-McFarland's ( $M$ - $M$ ) class of bent functions is the set of all the (bent) Boolean functions on  $\mathbb{Z}_2^{2n} = \{(\mathbf{x}, \mathbf{y}) | \mathbf{x}, \mathbf{y} \in \mathbb{Z}_2^n\}$  of the form

$$f(\mathbf{x}, \mathbf{y}) = \mathbf{x} \cdot \phi(\mathbf{y}) \oplus g(\mathbf{y}), \quad (2)$$

where  $\phi$  is any permutation of  $\mathbb{Z}_2^n$  and  $g \in \mathcal{B}_n$ .

Let  $f \in \mathcal{B}_n$ . If there exists an even integer  $0 \leq r \leq n$ , such that  $\|\{\boldsymbol{\omega} | \mathcal{W}_f(\boldsymbol{\omega}) \neq 0, \boldsymbol{\omega} \in \mathbb{F}_2^n\}\| = 2^r$ , where  $\|\cdot\|$  denotes the size (cardinality) of a set, and  $(\mathcal{W}_f(\boldsymbol{\omega}))^2$  equals  $2^{2n-r}$  or 0, for every  $\boldsymbol{\omega} \in \mathbb{F}_2^n$ , then  $f$  is called an  $r$ -order *plateaued* function in  $n$  variables. If  $f$  is a  $2\lceil(n-2)/2\rceil$ -order plateaued function in  $n$  variables, then  $f$  is also called a *semibent* function.

Let  $f \in \mathcal{GB}_n^8$  be as

$$f(\mathbf{x}) = v_0(\mathbf{x}) + v_1(\mathbf{x}) \cdot 2 + v_2(\mathbf{x}) \cdot 2^2, \quad (3)$$

where  $v_i(\mathbf{x}) \in \mathcal{B}_n, i = 0, 1, 2$ .

In [9, Theorem 19], Stănică et al. presented a sufficient and necessary condition for a function  $f$  as in (3) to be gbent.

**Theorem 2** ([9]). Let  $f \in \mathcal{GB}_n^8$  be as in (3). The following are true:

(i) If  $n$  is even, then  $f$  is gbent if and only if  $v_2, v_0 \oplus v_2, v_1 \oplus v_2, v_0 \oplus v_1 \oplus v_2$  are all bent, and  $\mathcal{W}_{v_0 \oplus v_2}(\mathbf{u})\mathcal{W}_{v_1 \oplus v_2}(\mathbf{u}) = \mathcal{W}_{v_2}(\mathbf{u})\mathcal{W}_{v_0 \oplus v_1 \oplus v_2}(\mathbf{u})$  for all  $\mathbf{u} \in \mathbb{Z}_2^n$ ;

(ii) If  $n$  is odd, then  $f$  is gbent if and only if  $v_2, v_0 \oplus v_2, v_1 \oplus v_2, v_0 \oplus v_1 \oplus v_2$  are all semibent, and  $\mathcal{W}_{v_0 \oplus v_2}(\mathbf{u}) = \mathcal{W}_{v_2}(\mathbf{u}) = 0$  and  $|\mathcal{W}_{v_1 \oplus v_2}(\mathbf{u})| = |\mathcal{W}_{v_0 \oplus v_1 \oplus v_2}(\mathbf{u})| = 2^{\frac{n+1}{2}}$ ; or,  $|\mathcal{W}_{v_0 \oplus v_2}(\mathbf{u})| = |\mathcal{W}_{v_2}(\mathbf{u})| = 2^{\frac{n+1}{2}}$  and  $\mathcal{W}_{v_1 \oplus v_2}(\mathbf{u}) = \mathcal{W}_{v_0 \oplus v_1 \oplus v_2}(\mathbf{u}) = 0$ , for all  $\mathbf{u} \in \mathbb{Z}_2^n$ .

From the above theorem, we know that the sufficient conditions that a function  $f$  as in (3) is gbent are abstract. Hence, we provide some sufficient conditions for a function  $f$  as in (3) to be gbent.

**Theorem 3.** Let  $n$  be an even integer,  $v_0, v_1, v_2 \in \mathcal{B}_n$  and  $f \in \mathcal{GB}_n^8$  be as in (3). The following  $v_0, v_1, v_2$  satisfy the sufficient conditions of Theorem 2 for the even case.

(i) Let  $v_0, v_1, v_2$  be bent functions and  $v_2, v_0 \oplus v_2, v_1 \oplus v_2, v_0 \oplus v_1 \oplus v_2$  be all bent, and  $(v_0 \oplus v_2)(\mathbf{x}) = \tilde{v}_0(\mathbf{x}) \oplus \tilde{v}_2(\mathbf{x})$ ,  $(v_1 \oplus v_2)(\mathbf{x}) = \tilde{v}_1(\mathbf{x}) \oplus \tilde{v}_2(\mathbf{x})$ ,  $(v_0 \oplus v_1 \oplus v_2)(\mathbf{x}) = \tilde{v}_0(\mathbf{x}) \oplus \tilde{v}_1(\mathbf{x}) \oplus \tilde{v}_2(\mathbf{x})$ .

(ii) Let  $v_2 \in \mathcal{B}_n$  be a bent function,  $v_0 = v_1$  and  $v_0 \oplus v_2$  be bent.

(iii) Let  $v_0(\mathbf{x}) = \mathbf{a}_0 \cdot \mathbf{x}$  and  $v_1(\mathbf{x}) = \mathbf{a}_1 \cdot \mathbf{x}$  respectively, be two linear functions. Let  $v_2 \in \mathcal{B}_n$  be a bent function, and  $\tilde{v}_2(\mathbf{x}) \oplus \tilde{v}_2(\mathbf{x} \oplus \mathbf{a}_0) \oplus \tilde{v}_2(\mathbf{x} \oplus \mathbf{a}_1) \oplus \tilde{v}_2(\mathbf{x} \oplus \mathbf{a}_0 \oplus \mathbf{a}_1) = 0$ .

**Table 1** Form of gbent functions comparison

Number of variables	$q$	From	Resource
$n + 2$	2	$h(\mathbf{x}, \mathbf{y}) = f(\mathbf{x}) \oplus (y_1 \oplus y_2)g(\mathbf{x}) \oplus y_1 y_2$	Ref. [10]
$n + 2$	Even integer	$h(\mathbf{x}, \mathbf{y}) = f(\mathbf{x}) + (y_1 \oplus y_2)g(\mathbf{x}) + \frac{q}{2}y_1 y_2$	Ref. [9]
$n + m$	Even integer	$h(\mathbf{x}, \mathbf{y}) = f(\mathbf{x}) + \frac{q}{2}(\mathbf{c} \cdot \mathbf{y})g_{\mathbf{c} \cdot \mathbf{y}}(\mathbf{x}) + \frac{q}{2}\vartheta(\mathbf{y})$	New

(iv) Let  $v_0(\mathbf{x}) = \mathbf{a}_0 \cdot \mathbf{x}$ , be a linear function. Let  $v_2 \in \mathcal{B}_n$  be a bent function,  $v_1 \oplus v_2$  be bent and  $\tilde{v}_2(\mathbf{x}) \oplus \tilde{v}_2(\mathbf{x} \oplus \mathbf{a}_0) \oplus (v_1 \oplus v_2)(\mathbf{x}) \oplus (v_1 \oplus v_2)(\mathbf{x} \oplus \mathbf{a}_0) = 0$ .

We now discuss the case when  $n$  is odd. Let  $n$  be a positive odd integer and  $g_1, g_2 \in \mathcal{B}_n$ . We say that  $g_1$  and  $g_2$  are *complementary semibent functions* in  $n$  variables if they are semibent (that is,  $(n - 1)$ -order plateaued) functions and satisfy the property that  $\mathcal{W}_{g_1}(\omega) = 0$  if and only if  $\mathcal{W}_{g_2}(\omega) \neq 0$ .

**Lemma 3.** Let  $n$  be an even integer and  $f \in \mathcal{B}_n$ . Then  $f$  is bent if and only if the two functions on  $\mathbb{Z}_2^{n-1}$ ,  $f(x_1, \dots, x_{j-1}, 0, x_{j+1}, \dots, x_n)$  and  $f(x_1, \dots, x_{j-1}, 1, x_{j+1}, \dots, x_n)$ , are complementary semibent functions on  $\mathbb{Z}_2^{n-1}$ , where  $j = 1, \dots, n$ .

**Theorem 4.** Let  $k, n$  be two integers and  $n = 2k - 1$ . Let  $\varphi = (\varphi_1, \dots, \varphi_k), \phi = (\phi_1, \dots, \phi_k)$  be Boolean maps from  $\mathbb{Z}_2^k$  to  $\mathbb{Z}_2^k$  such that both  $\phi$  and  $\phi \oplus \varphi = (\phi_1 \oplus \varphi_1, \dots, \phi_k \oplus \varphi_k)$  are permutations on  $\mathbb{Z}_2^k$ . Set  $\Delta_j = \{\phi(\mathbf{y}) | \mathbf{y} \in \mathbb{Z}_2^{j-1} \times \{0\} \times \mathbb{Z}_2^{k-j}\}$ ,  $\mathbf{y}_\epsilon^{(j)} = (y_1, \dots, y_{j-1}, \epsilon, y_{j+1}, \dots, y_k)$ , where  $\epsilon \in \mathbb{Z}_2, j = 1, 2, \dots, k$ . Let  $f \in \mathcal{GB}_n^8$  be as in (3), and let  $v_0(\mathbf{x}, \mathbf{y}_0^{(j)}) = \mathbf{a}_0 \cdot \mathbf{x} \oplus \varphi(\mathbf{y}_0^{(j)}) \cdot \mathbf{x}$ ,  $v_1(\mathbf{x}) = (\phi(\mathbf{y}_0^{(j)}) \oplus \phi(\mathbf{y}_1^{(j)})) \cdot \mathbf{x} \oplus g(\mathbf{y}_0^{(j)}) \oplus g(\mathbf{y}_1^{(j)})$  and  $v_2(\mathbf{x}) = \phi(\mathbf{y}_0^{(j)}) \cdot \mathbf{x} \oplus g(\mathbf{y}_0^{(j)})$ , where  $\mathbf{a}_0 \in \mathbb{Z}_2^k$ . If there exists one positive integer  $\varrho (\leq k)$  such that

$$\{(\phi \oplus \varphi)(\mathbf{y}) | \mathbf{y} \in \mathbb{Z}_2^{\varrho-1} \times \{0\} \times \mathbb{Z}_2^{k-\varrho}\} = \Delta_\varrho \quad (4)$$

(if  $\mathbf{a}_0 \neq \mathbf{0}_k$  we further require  $\Delta_\varrho$  to be a linear subspace of  $\mathbb{Z}_2^k$  and  $\mathbf{a}_0 \in \Delta_\varrho$ ), then  $v_0, v_1, v_2$  satisfy the conditions of Theorem 2 for the odd case, that is,  $f$  is gbent.

**Acknowledgements** This work was supported by National Natural Science Foundation of China (Grant Nos. 61303263, 61309034), and in part by Fundamen-

tal Research Funds for the Central Universities (Grant No. 2015XKMS086), and in part by China Postdoctoral Science Foundation Funded Project (Grant No. 2015T80600).

**Supporting information** The supporting information is available online at [info.scichina.com](http://info.scichina.com) and [link.springer.com](http://link.springer.com). The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

## References

- Rothaus O S. On ‘bent’ functions. J Combin Theory A, 1976, 20: 300–305
- Carlet C. Two new classes of bent functions. In: Proceedings of Workshop on the Theory and Application of Cryptographic Techniques, Lofthus, 1994. 77–101
- Zhang F, Wei Y, Pasalic E. Constructions of bent-negabent functions and their relation to the completed Maiorana-McFarland class. IEEE Trans Inf Theory, 2015, 61: 1496–1506
- Zhang W G, Xiao G Z. Constructions of almost optimal resilient Boolean functions on large even number of variables. IEEE Trans Inf Theory, 2009, 55: 5822–5831
- Zhang W G, Jiang F Q, Tang D. Construction of highly nonlinear resilient Boolean functions satisfying strict avalanche criterion. Sci China Inf Sci, 2014, 57: 049101
- Schmidt K U. Quaternary constant-amplitude codes for multicode CDMA. IEEE Trans Inf Theory, 2009, 55: 1824–1832
- Solé P, Tokareva N. Connections between quaternary and binary bent functions. <http://eprint.iacr.org/2009/544.pdf>
- Stănică P, Gangopadhyay S, Chaturvedi A, et al. Nega-Hadamard transform, bent and negabent functions. In: Proceedings of 6th International Conference on Sequences and Their Applications, Paris, 2010. 359–372
- Stănică P, Martinsen T, Gangopadhyay S, et al. Bent and generalized bent Boolean functions. Des Codes Cryptogr, 2013, 69: 77–94
- Zhao Y, Li H L. On bent functions with some symmetric properties. Discret Appl Math, 2006, 154: 2537–2543